	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	04-02		2/17/07	12/12/05	Page 1 of 6
State of Rhode Island Department of Administration Division of Information Technology		TITLE	Wireless Access		

1. Overview

It is recognized that wireless networking could offer great benefits to the State of Rhode Island in the pursuit of its primary objective of serving the public. Wireless networking has been in existence for a few years, but is still a relatively new technology. The recent ratification of further 802.11 standards for wireless access will continue to enhance interest in the technology. The growing availability of relatively inexpensive 'consumer-oriented' wireless technology and their apparent ease of installation could lead to an unacceptable, uncoordinated and unplanned growth of wireless networking on the campus.

It can no longer be acceptable practice to be allowed to install or operate wireless devices on the state network without a clear and agreed policy outlining the roles and responsibilities of all parties. These roles not only include the installation and setup of such network devices but also their ongoing use.

The design of wireless networks, specifically the placement of wireless access points to maximize coverage area and to minimize interference with other access points or devices and the issue of network security, is something that has to be addressed and planned at a campus wide level. Security of wireless networks is always a major concern and requires adherence to policy and full cooperation when wireless networking is incorporated into a network infrastructure.

This policy aims to set out a framework to deal with these issues. The intention of this policy is to define roles and responsibilities for the design of any emerging wireless network, the installation, registration and management of wireless access points, adequate management and allocation of the wireless frequency spectrum and the services offered to end users for wireless access.

2. Statement of Authority and Scope

This policy applies to all wireless network devices utilizing the Department of Administration's IP space including private non-routable IP space within the State's networks and all users of such devices. It covers all wireless connections to the network backbone, frequency allocation, network address assignment, registration in the Domain Name System, and services provided over wireless connections to end users both to and from the campus network.

Division of Information Technology (DoIT) is responsible for the operation and management of State's network infrastructure. A natural extension to the fixed network currently in existence is a wireless network. In order to ensure reliability, integrity, interoperability and security between the wired and wireless domains it is the responsibility of DoIT to ensure the design, management and appropriate use of the State's wireless infrastructure is in accordance with best practice and existing policies.

3. Definitions

Wireless networking is a relatively new technology so some definitions will aid in clarification of the policy.

- **Wireless Network:** The network technology that uses radio frequency spectrum to connect computing devices to a wired port on the State network. Common technologies are IEEE 802.11a, 802.11b and 802.11g. Bluetooth is as similar technology.
- **Wireless Infrastructure**: The wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless network
- **Base Station**: A network device that serves as a common connection point for devices in a wireless network. Access points use wireless antennas instead of wired ports for access by multiple users of the wireless network. Access points are shared bandwidth devices and are usually connected to the wired network.
- **Access point**: Same as **Base Station**.
- **Coverage:** The physical area where a level of wireless connectivity is available.
- **Channel:** The chosen frequency for communication between the end point and the base station.
- **RF Interference:** The degradation of a wireless communication signal caused by electromagnetic radiation from another source. Interference can slow down or eliminate a wireless transmission depending on the strength of the interfering signal.
- **Security**: The condition that provides for the confidentiality of data transmitted over a wireless network.
- **SSID:** Service Set Identifier, essentially a name that identifies a wireless network. All devices on a specific wireless network must know the SSID of that network.
- **Client hardware/software**: The equipment and software that is installed in a desktop, laptop, handheld, portable, or other computing device.

4. Rationale

There would be three major risks with an ongoing ad-hock deployment of wireless networks in the state network.

1. **Security**: By their very nature wireless LANs are open to anyone within range of the access point. Physical boundaries are no longer relevant. If a wireless access point is connected to the campus network without restrictions anyone with the proper equipment will be able to access the network. Furthermore, anyone with the proper equipment can spy on traffic. They can see users' passwords as well as other data. In line with other policies being introduced in this area security of wireless installations has to be rigorously managed.
2. **RF Interference**: There is a finite amount of bandwidth available for wireless use. The most common wireless LAN technology (802.11b) defines only 3 (or possibly 4) channels for effective use. If wireless LANs are installed without coordination with others in the area, interference is likely. This may result in significantly degraded performance for everyone.
3. **Equipment Diversity:** All standards compliant wireless equipment from reputable manufacturers will coexist with each other even leaving aside possible interpretations in the standard. However for a campus wide wireless LAN infrastructure to be properly planned, implemented and managed appropriate hardware needs to be chosen for deployment. Low cost 'consumer-oriented' devices which do not provide the management capabilities for campus wide networks should be avoided in flavor of more appropriate equipment.

5. Roles and Responsibilities

The objective is to define a framework where DoIT works with departments and faculties to enable the deployment and ongoing management of a wireless network infrastructure. The intention is not to restrict or constrain the growth of the network.

DoIT shall act as overall coordinators and controllers of the network. Individual departments and Agency IT Managers within those departments shall, where appropriate, be responsible for the localized management and implementation of the access points and infrastructure.

6. The Policy

6.1 Wireless base stations must abide by all national regulations pertaining to wireless devices. Furthermore base stations shall conform to recommended minimum specifications as defined by DoIT. Individuals and departments are expected to purchase in line with State purchasing policy and by seeking guidance from DoIT.

6.2 No wireless base stations are allowed to be connected to the state network without prior registration with DoIT. Wireless equipment is essentially no different to any other network host so must adhere to the policy.

6.3 The locations of and an official point of contact for all wireless access points must be registered with the DoIT service desk. Ideally at least one point of contact will be the official IT supporter for the department who may act as an official representative for a more senior official if that is seen to be required.

6.4 Allocation of channels, SSID and encryption standards must be agreed and authorized before deployment.

6.5 ALL wireless LAN communications shall be encrypted.

6.6 All wireless communication shall require user authentication before granting access to campus network and beyond.

6.7 Wireless networks must be designed and deployed to avoid any interference between competing devices in the electro magnetic spectrum. Other devices may mean neighboring wireless base stations or other components using the radio spectrum such as cordless telephones or competing technologies. In the event that a wireless device interferes with other equipment the local department should be expected to resolve the situation. Disputes over channel allocation should be handled by the official point of contact for that base station. Where multiple units or departments are involved Computing Services will act as arbiter or coordinator.

6.8 Physical security should be considered the joint responsibility of all parties when planning the location of wireless access point and other wireless network components.

7. Conformance with Existing Policies

DoIT is authorized to take whatever reasonable steps are necessary to ensure compliance with this, and other network related policies that are designed to protect the integrity and security of the state network. Specific attention is drawn to the IT Security policy.

Due to the nature of wireless networks the following should also be noted:

Authorization to disconnect any wireless network on state network which poses a security threat.

> If a serious security breach is in process DoIT may disconnect the LAN immediately. Every reasonable attempt will be made beforehand to reach the registered 'point of contact' to resolve security problems. Computing Services shall also have the authority to disconnect any wireless network from the campus network backbone whose traffic patterns seem unusually suspicious or violates practices set forth in this and other policies.

It is the responsibility of the department, center or unit to be knowledgeable regarding the provision all Computing Services policies.

8. Grievance and Appeals

Grievances with this policy or conflicts or disputes between DoIT and any department, center or unit should be directed to the Director of Operations for resolution.

9. APPROVALS

Walter Casper

Assistant Director of Planning, Policy & Technology

2/17/07

Date

Director of Operations

2/16/07

Date

Chief Information Officer

2/20/07

Date

Director, Department of Administration

Date